IDA INSTITUTE FOR DEFENSE ANALYSES

NSD-5324

# Exposure: A New Decision Metric for Selecting Effective Sets of Security Upgrades

Kevin E. Burns
Jason A. Dechant
J. Darrell Morgeson
Yazmin Seda-Sanabria
Enrique E. Matheu

January 2015

Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, Virginia  22311-1882

IDA Log No. H 14-001136

**About This Publication**

**The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.**

**Copyright Notice**

**4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.**

NSD-5324

# Exposure: A New Decision Metric for Selecting Effective Sets of Security Upgrades

Kevin E. Burns
Jason A. Dechant
J. Darrell Morgeson
Yazmin Seda-Sanabria
Enrique E. Matheu

January 2015

# EXPOSURE: A NEW DECISION METRIC FOR SELECTING EFFECTIVE SETS OF SECURITY UPGRADES

Kevin E. Burns, PhD[1]
James D. Morgeson[2]
Jason A. Dechant, PhD[3]
Yazmin Seda-Sanabria[4]
Enrique E. Matheu, PhD[5]

## ABSTRACT

The United States Army Corps of Engineers (USACE) conducts Security Risk Assessments (SRAs) at its most consequential dam projects. The Common Risk Model for Dams (CRM-D) provides a mathematically rigorous and easy-to-implement way to conduct SRAs. The CRM-D quantifies risk as the product of the probability of a successful attack, given it is attempted, and consequences. Referred to as *conditional risk*, this decision metric is the expected loss given a specified attack is attempted on a particular target. A specified attack (consisting of an attacker type and an attack vector) carried out on a particular target comprises a scenario.

The CRM-D considers three attacker types and thirty-two attack vectors identified by USACE Headquarters (HQs). A dam with only a modest number of critical assets could thus have several hundred scenarios and, consequently, several hundred conditional risk estimates. This paper introduces a decision metric, *exposure*, which allows the analyst to aggregate conditional risk estimates across scenarios. The analyst can use exposure to compare risks by attack type, by target or for any useful set of scenarios. These comparisons can guide an analyst in determining a proposed set of security upgrades. A standard set of graphics and return-on-investment calculations based on exposure are introduced that summarize the current level of risk at a dam project as well as the reduced level of risk should the set of recommended security upgrades be implemented.

## INTRODUCTION

In 2005, the Institute for Defense Analyses (IDA) initiated the development of the Common Risk Model (CRM) for evaluating and comparing risks associated with the Nation’s critical infrastructure. This model incorporates commonly used risk metrics that are designed to be transparent, simple, and mathematically justifiable. The CRM also

[1] Research Staff Member, Strategy Forces, and Resources Division (SFRD), Institute for Defense Analyses (IDA), Alexandria, VA 22311, kburns@ida.org.

[2] Research Staff Member, SFRD, IDA, Alexandria, VA 22311, jmorgeso@ida.org.

[3] Research Staff Member, SFRD, IDAs, Alexandria, VA 22311, jdechant@ida.org.

[4] National Program Manager, Critical Infrastructure Protection & Resilience Program Office of Homeland Security, Directorate of Civil Works, U.S. Army Corps of Engineers, Washington, DC 20314, Yazmin.Seda-Sanabria@usace.army.mil.

[5] Sector Outreach and Programs Division, Office of Infrastructure Protection, National Protection and Programs Directorate, U.S. Department of Homeland Security, Washington, DC 20598, Enrique.Matheu@hq.dhs.gov.

enables comparisons of risks to critical assets both within and across critical infrastructure sectors.

Over the past few years, an extended version of the CRM has been under development by IDA in collaboration with the USACE and the U.S. Department of Homeland Security (DHS). The extended model—Common Risk Model for Dams (CRM-D)—takes into account the unique features of dams and navigation locks and provides a systematic approach for evaluating and comparing risks from terrorist threats across a large portfolio[6] (Seda-Sanabria et al., 2011a).

In general, the risk for an attack scenario is considered to be a function of three variables: *threat*—the likelihood of an attack scenario being chosen by adversaries; *vulnerability* —the likelihood of defeating the target's defenses, given that the attack is chosen; and estimated *consequences* of the attack, given the target's defenses are defeated (DHS 2013*)*. Therefore, it can be stated that

$$R = f\,(T, V, C), \tag{1}$$

where R is risk, T is threat, V is vulnerability, and C is the consequences. A widely used approach is to define the risk function as the product of these three variables:

$$R = T \text{ x } V \text{ x } C. \tag{2}$$

Threat, denoted as P(A), is defined as the probability that a given attack scenario is chosen, *conditional* on one of the attack scenarios in the portfolio being chosen within a specified timeframe (usually taken to be a year). Vulnerability is defined as the conditional probability that a given attack vector will successfully defeat the target's defenses, given the attack scenario is chosen, or P(S|A). Consequences, denoted as C, are defined in terms of lives lost and economic loss given that the attack successfully breaches all of the defenses protecting the scenario target. Thus

$$R = P(A) \text{ x } P(S|A) \text{ x } C. \tag{3}$$

One can also define conditional risk for a scenario, $R_C$:

$$R_C = V \text{ x } C = P(S|A) \text{ x } C. \tag{4}$$

$R_C$ is conditional on the adversary's choice of a specific scenario. Calculating conditional risks for all scenarios can be useful to an analyst at a dam project as this knowledge can inform decisions regarding how to improve the security measures at the dam's facility. The next section provides an overview of how conditional risk is estimated in CRM-D.

[6] A portfolio is a set of dam projects evaluated by a risk analyst.

## BASIC CONCEPTS: THE COMMON RISK MODEL FOR DAMS

A conceptually simple model of layered defenses is used to evaluate the conditional risk of a given critical infrastructure target. As an example, Figure 1 represents the case of a target protected by three notional defensive layers.

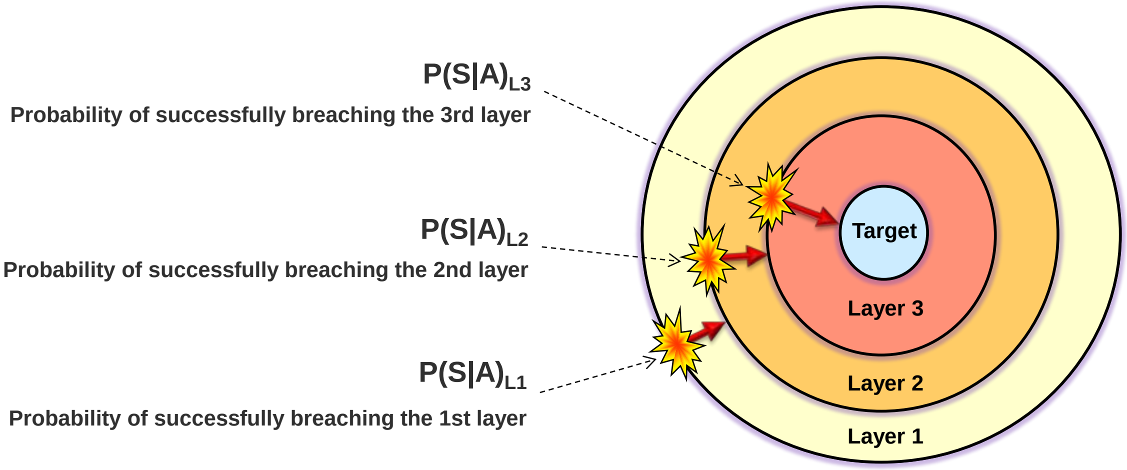
$P(S|A)_{L3}$
Probability of successfully breaching the 3rd layer
$P(S|A)_{L2}$
Probability of successfully breaching the 2nd layer
$P(S|A)_{L1}$
Probability of successfully breaching the 1st layer
Target
Layer 3
Layer 2
Layer 1

**Figure 1. Conceptual Model of Layered Defenses**

For the target to be successfully attacked, each defensive layer providing some form of protection would need to be successfully breached. For the case shown in Figure 1, the joint probability that a given attack, if attempted, will be successful in reaching the target, considering it being attempted (also known as the vulnerability or P(S|A)), can be determined using the following expression:[7]

$$P(S|A) = P_{L1} \text{ x } P_{L2} \text{ x } P_{L3.} \qquad (5)$$

As part of the CRM-D development, a representative set of physical attack vectors was defined by USACE HQ to represent a wide spectrum of attacks that can be used to facilitate the comparison of vulnerability and conditional risk results across a large portfolio. These attack vectors,[8] which assume high-capability adversaries (well-trained attackers with significant access to resources), are listed in Table 1 and are arranged by categories known as *attack types*. The twenty-eight attack vectors listed in Table 1 are a subset of the thirty-two total attack vectors defined by USACE HQ for various adversary types.

[7] The CRM-D model explicitly accounts for time delays in the attack due to the time it takes to breach layers and the time it takes to traverse interlayer distance. Also taken into account is attack vector degradation due to armed defenders. Since these are factors normally used in the estimation of conditional probabilities, CRM-D simplifies the calculation of conditional probabilities by assuming independence among the probability estimates except for those factors explicitly accounted for. See Morgeson et al., “Incorporating Uncertainties in Estimation of Vulnerabilities for Security Risk Assessments.”

[8] The attack vectors used in CRM-D can be extended to include additional attack vectors that are identified over time.

Table 1. Attack Vectors Considered for High-Capability Adversaries

| Attack Mode | Attack Type | Attack Vectors | | | |
|---|---|---|---|---|---|
| Land | VBIED | Sedan | Cargo Van | Box Truck | Large Truck |
| | Assault Team | Single Attacker | Small-Size Cell | Medium-Size Cell | Large-Size Cell |
| | Stand-off Weapon | Large-Caliber Rifle | Rocket-Propelled Grenade | Mortar | Man-portable Guided Missile |
| | Sabotage | Insider | Outsider | - | - |
| | Excavating Attack | Mechanical | Kinetic | - | - |
| Water | Water-borne Improvised Explosive Device (WBIED) | Inflatable Boat | Small Boat | Large Boat | Barge |
| | Underwater IED | Surface Swimmer | Subsurface Swimmer | Modified Small Boat | Semi-submersible Boat |
| Air | Impact | Helicopter | Small Airplane | Narrow-body Airliner | Wide-body Airliner |

The probability that a specific attack vector would be successful in reaching a given target depends on the probability that each of the defensive layers sequentially encountered along the attack path is successfully penetrated. These individual layer probabilities, in turn, depend on the type of adversary, the attack vector chosen, and the strength of the defenses at the particular layer (Morgeson 2013). To illustrate the concept, assume that a given target T-1 is protected by three defensive layers ($L_1$, $L_2$, and $L_3$). For a given attack vector denoted as AV-1, the overall probability of success for the scenario defined by attack vector AV-1 and the target T-1 is the joint probability of successfully penetrating all three layers. For this scenario, equation 5 can be written using the following notation:

$$P(S|A)_{\text{Overall}} = P(S|A)_{\text{AV-1, L1}} \text{ x } P(S|A)_{\text{AV-1, L2}} \text{ x } P(S|A)_{\text{AV-1, L3.}} \qquad (6)$$

Equation 7 is an example of the calculation in equation 6 using notional estimates for the probabilities for each layer.

$$P(S|A)_{\text{Overall}} = 0.2 \text{ x } 0.7 \text{ x } 0.9 = 0.126. \qquad (7)$$

As defined in equation 4, conditional risk is the product of the probability of successful attack (given that that attack is attempted) multiplied by the corresponding consequences.

For illustrative purposes, assume that the consequences of a successful attack on target T-1 is estimated to be $1 million (M), and therefore

$$R_C = P(S|A) \times C = 0.126 \times \$1M = \$126,000. \tag{8}$$

$R_C$ is the expected loss given a hypothetical attack on target T-1 protected by layers $L_1$, $L_2$, and $L_3$. Therefore, for every attack scenario (i.e., combination of an adversary type, a specific attack vector, and a given target), the CRM-D methodology provides a systematic approach to estimate conditional risk. Table 2 contains conditional risk calculations for a set of scenarios at a notional dam.

**Table 2. Conditional Risk for Selected Attack Scenarios for a Notional Dam**

| Attack Type | Attack Vector | Impoundment | | | | | Powerhouse (Control Center) | | | | | Powerhouse (Turbines and Generators) | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Conseq. | | $P(S\|A)_{FINAL}$ | Conditional Risk (Life) | Conditional Risk (Econ. $M) | Conseq. | | $P(S\|A)_{FINAL}$ | Conditional Risk (Life) | Conditional Risk (Econ. $M) | Conseq. | | $P(S\|A)_{FINAL}$ | Conditional Risk (Life) | Conditional Risk (Econ. $M) |
| | | Loss of Life | Economic Loss ($M) | | | | Loss of Life | Economic Loss ($M) | | | | Loss of Life | Economic Loss ($M) | | | |
| VBIED | Sedan | 1 | 1 | 1.0 | 1 | 1 | 11 | 1 | 1.0 | 11 | 1 | 1 | 22 | 1.0 | 1 | 22 |
| | Van | 1 | 3 | 1.0 | 1 | 3 | 11 | 3 | 1.0 | 11 | 3 | 1 | 22 | 1.0 | 1 | 22 |
| | Box Truck | 1 | 3 | 1.0 | 1 | 3 | 11 | 3 | 1.0 | 11 | 3 | 1 | 44 | 1.0 | 1 | 44 |
| | Large Truck | 100 | 200 | 1.0 | 100 | 200 | 11 | 3 | 1.0 | 11 | 3 | 1 | 66 | 1.0 | 1 | 66 |
| Assault Team | Single Attacker | 1 | 0 | 0.51 | 1 | 0 | 11 | 3 | 0.58 | 6 | 2 | 1 | 44 | 0.58 | 1 | 25 |
| | Small Cell | 1 | 0 | 0.9 | 1 | 0 | 11 | 3 | 0.81 | 9 | 2 | 1 | 132 | 0.81 | 1 | 107 |
| | Medium Cell | 1 | 1 | 1.0 | 1 | 1 | 11 | 3 | 1.0 | 11 | 3 | 1 | 132 | 1.0 | 1 | 132 |
| | Large Cell | 1 | 1 | 1.0 | 1 | 1 | 11 | 3 | 1.0 | 11 | 3 | 1 | 132 | 1.0 | 1 | 132 |

*Source*: The data in Table 2 and associated graphics throughout this paper are drawn from Michael Keleher, Steven Walser, and Samuel Himel, *The Common Risk Model for Dams Support System: A Prototype Analyst Tool* (Alexandria, VA: Institute for Defense Analyses, IDA Paper P-5220, to be published). Values in the table are rounded.

Note that Table 2 contains forty-eight conditional risk calculations (highlighted in red). Yet this represents only a fraction of conditional risk calculations that would be performed at many dams. This table includes only one adversary type, only two attack types (thus only eight attack vectors), and only three assets. The challenge facing a risk analyst is how to summarize the data contained in pages and pages of such tables in a way that informs decisions about potential security upgrades.

# INTRODUCING EXPOSURE

The purpose of calculating conditional risks for many scenarios is ultimately to help the decision maker understand how to reduce such risks most effectively by investing in security improvements. The goal is to compare risks among different target assets at a dam, for different types of attack vectors, or for different dams within a portfolio of dams. To make any of these comparisons, it is necessary to aggregate risks across scenarios. Conditional risk cannot be aggregated across scenarios because by definition, each conditional risk estimate is based on the adversary choosing that scenario. A different decision metric (other than conditional risk alone) is needed.

A decision metric is needed that retains the essential information contained in conditional risk for each scenario considered, but also quantitatively summarizes conditional risk across multiple scenarios in order to inform decision makers as they contemplate potential security upgrades. Because the metric is intended to inform decision makers, the metric should ideally be intuitive. This paper introduces such a metric: *exposure*.

## Defining Exposure

Exposure is defined as human lives and economic value at risk due to an attack. Exposure can be determined for any set of scenarios (including a single scenario) of interest to the analyst. Even when exposure is used as a summary metric for multiple scenarios, it is defined as human lives or economic value at risk due to *a* potential attack. Intuitively, the number of human lives at risk from a single attack at a specified dam cannot exceed the maximum number of lives lost considering all scenarios at that dam. Consequently, exposure, measured in terms of lives lost,[9] for any set of scenarios, will never exceed the maximum possible lives lost from any individual scenario in the set. For example, consider Table 3 which presents the consequences in terms of loss of life for selected scenarios at a notional dam. The largest loss of life from any single scenario is one hundred (for the scenario involving the large truck vehicle-borne improvised explosive device [VBIED] against the impoundment). Exposure for any subset of these scenarios (including exposure for *all* the scenarios in Table 3) will not exceed one hundred. The analyst can usefully compare exposure calculations by attack type or by asset or for any useful set of scenarios. The results of these comparisons guide a decision maker who is determining the most effective set of proposed security upgrades.

## Calculating Exposure

The considerations discussed in the previous section suggest calculating exposure for a set of scenarios as a weighted sum of the conditional risk estimates for each scenario in

[9] Exposure is defined and calculated both in terms of human lives and economic value. The calculations for human lives and economic value are always done separately, just as conditional risk calculations are made separately. In the examples throughout the paper, either human lives or economic value will be chosen to illustrate a particular point.

the set.[10] There are numerous weighting schemes[11] that an analyst could choose. Considering the previously stated goals of a metric that (1) preserves the essential information contained in conditional risk estimates and (2) is intuitive to decision makers, the authors propose the following method for calculating exposure. Exposure—denoted $R_C$'—for any set of scenarios, is the sum of scaled conditional risk for each scenario so that (1) the scaling factor for each scenario is the same and (2) the exposure for the set of all scenarios at an undefended dam (i.e., when P(S|A) equals 1.0 for each scenario) is equal to the consequences of the individual scenario that equals or exceeds the consequences of all other scenarios. (This value of consequences is referred to as $C_{MAX}$; see example below.)

A dam (considered as an aggregation of all the critical assets at the dam) cannot be more exposed, that is, suffer more than the worst consequences a given adversary type can impose in a single attack. The exposure for each scenario is its conditional risk multiplied by a scaling constant, denoted by "k." Scaling conditional risk allows for a realistic and valid comparison of conditional risks, both at a dam and among a portfolio of dams, without sacrificing the valuable information embedded in the conditional risk estimate. Exposure allows one to compare different sets of attack vectors or different assets at a dam. It also permits estimates of the relative values of different sets of security upgrades by observing the amount of reduction in exposure following the application of each set of security upgrades. Table 3 illustrates how exposure would be calculated for a set of scenarios at a notional dam. In Table 3,

- C indicates consequences, in loss of life for an individual scenario.
- $C_{TOTAL}$ is the sum of consequences for all scenarios considered in the table.
- $C_{MAX}$ is the largest C for an individual scenario under consideration in the table
- $k = C_{MAX}/C_{TOTAL}$.
- Exposure is denoted $R_C'$, and is calculated as $R_C' = k \times R_C$.
- $R_C'_{As\text{-}Is}$ indicates the exposure for a scenario, given the current security measures present at the dam project.

[10] The notion of aggregating/summarizing a collection of conditional risks, with each conditional risk tied to a distinctly unique conditioning event, may be considered analytically unsatisfying. Such a decision metric has no physical interpretation; nor does it have a stochastic interpretation, such as an expected value of loss. Nevertheless, it is a useful decision metric to decision makers because they must consider the magnitude of overall risk exposure and not isolated events.

[11] See discussion in this paper on alternative metrics.

**Table 3. Exposure (Loss of Life) for Selected Scenarios from a Notional Dam**

| Attack Type | Attack Vector | Target Asset | C | P(S\|A) | P(S\|A) x C = $R_C$ | k x $R_C$ = $R_C'_{As\text{-}Is}$ |
|---|---|---|---|---|---|---|
| $C_{TOTAL} = \Sigma C = 151$; $C_{MAX} = 100$; $k = C_{MAX}/C_{TOTAL} = 100/151 = 0.66$ | | | | | | |
| VBIED | Impoundment | | | | | |
| | Sedan | | 1 | 1.0 | 1.0 | 0.66 |
| | Van | | 1 | 1.0 | 1.0 | 0.66 |
| | Box Truck | | 1 | 1.0 | 1.0 | 0.66 |
| | Large Truck | | 100 | 1.0 | 100 | 66 |
| Assault Team | Control Center | | | | | |
| | Single Attacker | | 11 | .58 | 6.4 | 4.2 |
| | Small Cell | | 11 | .81 | 8.9 | 5.9 |
| | Medium Cell | | 11 | 1.0 | 11.0 | 7.3 |
| | Large Cell | | 11 | 1.0 | 11.0 | 7.3 |
| | Turbines and Generators | | | | | |
| | Single Attacker | | 1 | .58 | 0.58 | 0.38 |
| | Small Cell | | 1 | .81 | 0.81 | 0.53 |
| | Medium Cell | | 1 | 1.0 | 1.0 | 0.66 |
| | Large Cell | | 1 | 1.0 | 1.0 | 0.66 |

## USING EXPOSURE TO DEVELOP RISK MITIGATION OPTIONS

A Risk Mitigation Option (RMO) is a package of security upgrades intended to reduce exposure at critical assets and components of a dam project. The upgrades consist of improvements or additions to the defensive layers at the project. Options are constrained in practice by command guidance such as funding limitations or operational considerations.

The decision metric that will be used to evaluate potential RMOs is the net reduction in the exposure for the set of all scenarios considered at the project. Exposure for a dam in its current security configuration is denoted $R_C'_{As-Is}$. It is calculated using conditional risk estimates for each scenario based on the P(S|A) values for the current defensive configuration at each layer protecting the dam. $R_C'_{RMO}$ denotes exposure for the dam after implementing the proposed RMO. It is calculated using conditional risk estimates for each scenario based on revised P(S|A) values resulting from the proposed defensive configurations.

Exposure was introduced to help the analyst use conditional risk estimates to develop RMOs that effectively reduce risk. Exposure, calculated by summing scaled conditional risk values over different sets of scenarios, is particularly helpful in answering two questions from the dam owner/operator perspective:

1) Which targets are currently the most exposed?
2) Which attack vectors currently cause the most exposure?

The first question is addressed by calculating exposure for each asset at the dam. That is, calculate the sum of scaled conditional risk estimates over each scenario involving a particular asset. Similarly, the second question is addressed by calculating exposure for each attack type. That is, calculate the sum of scaled conditional risk estimates over each scenario involving a particular attack type. In the next section, graphics are introduced that help the analyst answer these two questions.

## Graphical Displays to Help Develop RMOs

Each scenario contributes to the overall exposure at a dam project. In order for an analyst to recommend security upgrades that efficiently reduce that level of exposure, it would be helpful to know which scenarios contribute the most to the overall level of exposure. As previously mentioned, this can be analyzed by asset or by attack type. Pie charts are an intuitive way to display this information.

Figures 2 through 4 show how exposure is distributed over assets and attack vectors for current defenses at a notional dam. Charts such as these inform the analyst during the process of building RMOs. $R_C'_{AS-IS}$ is calculated for the set of all scenarios; each wedge in the pie charts represents the percentage of that total that is contributed by the set of scenarios that only involve the asset (or attack type) indicated.

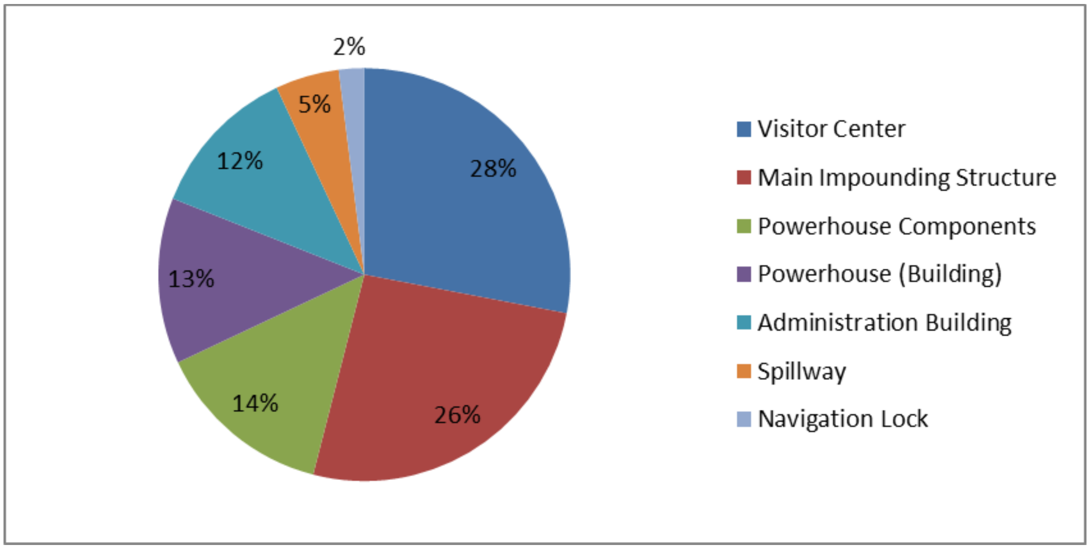

**Figure 2. Distribution of Loss-of-Life Exposure Over Assets for "As-Is" Defenses**

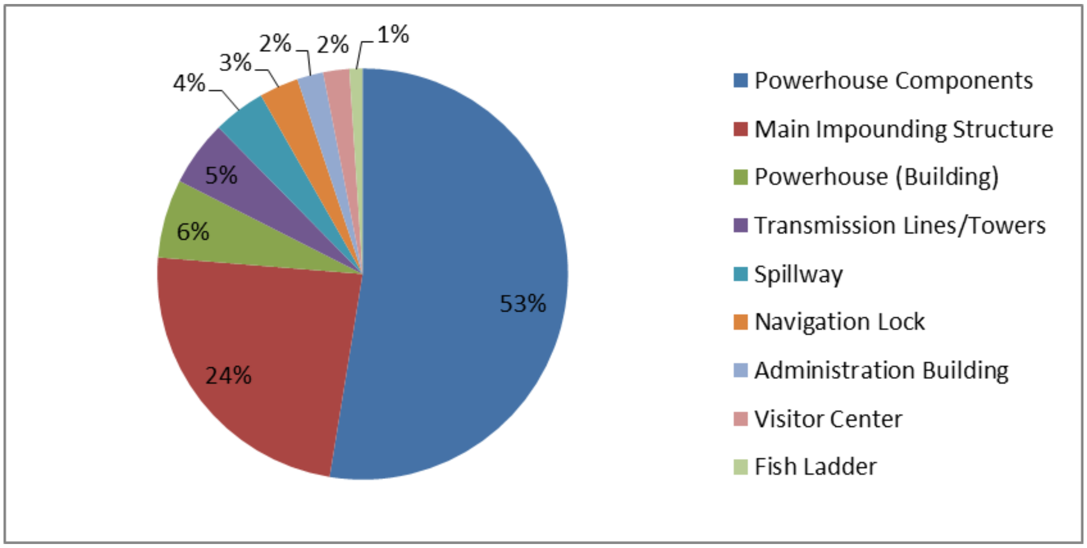

**Figure 3. Distribution of Economic Exposure Over Assets for "As-Is" Defenses**

Figures 2 and 3 both display relevant information to help answer the question, "Which targets are currently the most exposed?" Notice, for example, in Figure 3, the analyst and/or decision maker can see immediately that roughly three quarters of all *economic* exposure is contributed by scenarios involving only two assets—the components in the powerhouse and the main impounding structure. Figure 2, on the other hand, shows that the largest exposure in terms of loss of life is at the visitor center. These types of insights are invaluable to an analyst as he or she considers where to propose security upgrades at the dam project.

The same type of analysis can be conducted by attack type. Figure 4 helps answer the question, "Which attack vectors currently cause the most exposure?" It shows that roughly three quarters of total exposure at the project is attributed to scenarios involving VBIEDs and Assault Teams. An analyst can also readily surmise that protecting against land-based attacks is more likely to lower overall exposure than protecting against water-borne attacks.

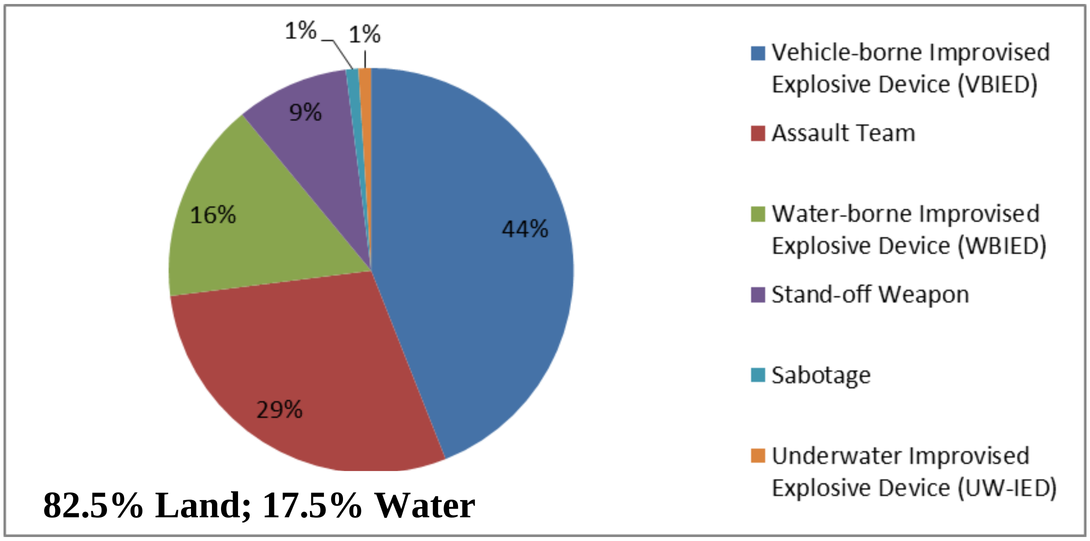

**Figure 4. Distribution of Loss-of-Life Exposure Over Attack Vector Types for "As-Is" Defenses**

## Graphical Displays that Help Evaluate RMOs

The pie charts in Figures 2, 3, and 4 aid the analyst in creating RMOs designed to better protect certain assets or to better protect against certain types of attacks where the dam is most exposed. The bar chart in Figure 5 quantifies the reduction in exposure that would be achieved if the proposed RMO is implemented. Figure 5 presents three calculations for total exposure at the project based on three different security configurations at the dam. The red bar, denoted $R_C{'}_{\text{Undefended}}$, represents the level of exposure if there were no effective defenses at the dam project, that is, the P(S|A) values for every scenario is 1.0. Mathematically, this means that $R_C$ equals consequences for every scenario. By construction, $R_C{'}$, in this case, is equal to the maximum consequence level over all scenarios. Including this calculation in the graphic allows the decision maker to readily observe the current state of defenses (represented by the height of the blue bar) vis-à-vis an undefended dam. The green bar represents the level of exposure if the proposed RMO was implemented. The percent reduction expressed at the top of the chart is a comparison of the exposure levels for the RMO and the current state of defenses.

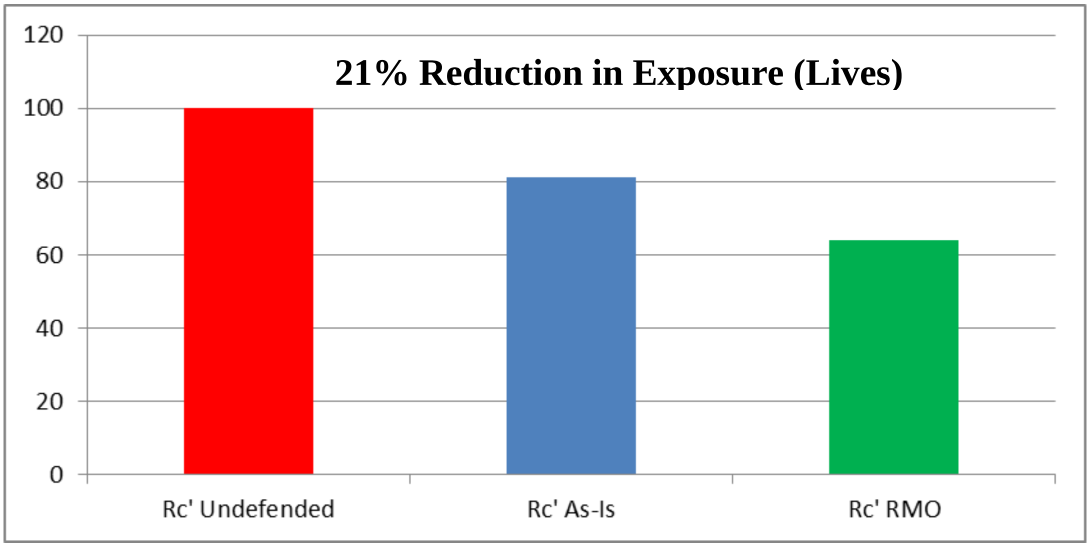

**Figure 5. Reduction in Loss-of-Life Exposure for RMO**

In this particular notional example, the decision maker can readily see that the proposed RMO would reduce exposure in terms of loss of human life by 9 percent.

### Implementing Exposure

IDA has created a training tool known as the Common Risk Model for Dams Support System (CRM-DSS). Among other things, this tool automates the calculation of exposure and the creation of all the graphics introduced in this paper. CRM-DSS has successfully been used to train thirty-five USACE analysts to conduct a Security Risk Assessment (SRA) based on exposure calculations. Analysts have used the tool to successfully complete SRAs at multiple dams.

## OTHER POTENTIAL METRICS

Exposure is a weighted sum of conditional risk estimates for a particular set of scenarios. It is not the only possible solution for the problem of summarizing conditional risk estimates across scenarios. Other weighted sums were considered; each has its own strengths and weaknesses. For developing individual SRAs at individual USACE dams, exposure was deemed to have the most desirable properties of various metrics that were considered. The following subsections present four alternative metrics along with a brief discussion of their merits and demerits.

### Summing Conditional Risk Estimates

Perhaps the most intuitive way to combine conditional risk estimates across a set of scenarios is to simply add the conditional risk estimates without weighting them. This solution has two significant disadvantages. Using this metric, the measure of risk attributed to a set of scenarios will always increase as scenarios are added to the set. Thus it is theoretically possible for one dam, say Dam A, to have a higher measure of risk than say Dam B simply because Dam A is vulnerable to more scenarios than Dam B, regardless of the potential consequences from any one scenario. The second disadvantage is related to the first. Using this metric, a dam could have a measure of risk that is larger than the possible consequences from any single attack.

## Maximum Possible Consequences

Another possible weighting scheme is to give the scenario with the largest consequences a weight of 1 and give all other scenarios a weight of 0. This appropriately places an emphasis on the largest consequence scenario but totally ignores all other scenarios. Imagine an RMO that recommends adding a water layer on the downstream side of the dam. This might significantly lower risk to a number of assets that can be attacked from the downstream side. However, if the largest consequence scenario can only be attacked from upstream, this RMO will not reduce the measure of risk at all if this metric is employed.

## Threat Estimate: P(A)

The CRM-D contains a module (Kirpichevsky 2012) that estimates the threat parameter, P(A) in equation (3). This parameter could be considered a weight on conditional risk and has some of the desirable properties of exposure. In fact, it has the added benefit of capturing the threat component of risk. However, the P(A) module was developed for use at the portfolio level.

## Average Conditional Risk

Another intuitive weighting scheme is to use the arithmetic average of the conditional risk estimates for all the scenarios in the set of interest, thus equally weighting each scenario. Initially, this metric seems to be more intuitive than exposure and might be more easily explained to decision makers. It is interesting to note that exposure is also a weighting scheme in which all the scenarios are equally weighted. The difference is that in exposure the weights do not necessarily sum to 1. The advantage of the weighting scheme used to calculate exposure is that it has a more intuitive interpretation, particularly in the case of an undefended dam. Consider for example the following notional situation depicted in Table 4. The level of exposure at the entire dam is 100, but the average conditional risk is 12.5. In this example, the average conditional risk is not a very descriptive measure of how exposed the dam is to attack, that is, how much is at risk. If more scenarios that have little or no conditional risk are added, the average conditional risk becomes a summary metric that is even less intuitive.

**Table 4. Exposure (Economic) for Select Scenarios from a Notional Dam**

| Attack Type | Attack Vector | Target Asset | C | P(S\|A) | P(S\|A) x C = $R_C$ | k x $R_C$ = $R_C{'}_{As\text{-}Is}$ |
|---|---|---|---|---|---|---|
| $C_{TOTAL} = \Sigma\ C = 200; C_{MAX} = 100; k = C_{MAX}/C_{TOTAL} = 100/200 = 0.5$ | | | | | | |
| VBIED | Impoundment | | | | | |
| | Sedan | | 20 | 1.0 | 20 | 10 |
| | Van | | 30 | 1.0 | 30 | 15 |
| | Box Truck | | 50 | 1.0 | 50 | 25 |
| | Large Truck | | 100 | 1.0 | 100 | 50 |
| Assault Team | Impoundment | | | | | |
| | Single Attacker | | 0 | 1.0 | 0 | 0 |
| | Small Cell | | 0 | 1.0 | 0 | 0 |
| | Medium Cell | | 0 | 1.0 | 0 | 0 |
| | Large Cell | | 0 | 1.0 | 0 | 0 |

## CONCLUSION

Exposure is an intuitive concept that provides risk analysts with a method for synthesizing conditional risk calculations across multiple scenarios that is easy to calculate. The synthesis of condition risk calculations at an individual dam provided by this new metric can be presented to decision makers via graphical displays that are informative and easy to comprehend. It has been successfully tested in training courses and in actual SRAs conducted at USACE dams.

## REFERENCES

Dechant, Jason A., John L. Conley, Anthony M. Fainberg, David R. Goodman, Anthony C. Hermes, Michael J. Keleher, Kevin F. McCrohan, and J. Darrell Morgeson. 2012. *The Common Risk Model for Dams: Methodology and Application*. IDA Paper P-4761. Alexandria, VA: IDA.

Keleher, Michael J., Steven Walser, and Samuel Himel. To be published. *The Common Risk Model for Dams Support System: A Prototype Analyst Tool.* IDA Paper P-5220. Alexandria, VA: IDA.

Kirpichevsky, Yev, Jason A. Dechant, Victor A. Utgoff, J. Darrell Morgeson, Colin M. Doyle, and Anton V. Strezhnev. 2012. *Estimating Threat from Adaptive Adversaries: Probabilistic Decision Modeling in the Common Risk Model for Dams.* IDA Paper P-4857. Alexandria, VA: IDA.

Morgeson, J. Darrell, Yazmin Seda-Sanabria, E. E. Matheu,  and Michael J. Keleher. 2013. “Incorporating Uncertainties in Estimation of Vulnerabilities for Security Risk Assessments.” Proceedings 33rd USSD Annual Meeting and Conference, Phoenix, Arizona, February 11–15, 2013.

National Research Council. 2010. *Review of the Department of Homeland Security's Approach to Risk Analysis.* Washington, DC: The National Academies Press.

Seda-Sanabria, Y., M. A. Fainberg, and E. E. Matheu. 2011a. “A Consistent Approach for Vulnerability Assessment of Dams.” Proceedings 31st USSD Annual Meeting and Conference, San Diego, California, April 11–15, 2011.

Seda-Sanabria, Y., M. A. Fainberg, E. E. Matheu, J. D. Tressler, and M. L. Bowen. 2011b. “Implementation of the Common Risk Model for Dams for Security Assessments of USACE Critical Infrastructure.” Proceedings Dam Safety 2011 Conference, Washington, DC, September 25–29, 2011.

U.S. Department of Homeland Security. 2013. *National Infrastructure Protection Plan*: *Partnering for Critical Infrastructure Security and Resilience*. Washington, DC: DHS. Available at http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

U.S. Government Accountability Office. 2005. “Risk Management.” GAO-06-91. Washington, DC: GAO. Available at www.gao.gov/cgi-bin/getrpt?GAO-06-91.

## REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*

**1. REPORT DATE (DD-MM-YY)**
January 2015

**2. REPORT TYPE**
Final

**3. DATES COVERED (From – To)**

**4. TITLE AND SUBTITLE**
Exposure: A New Decision Metric For Selecting Effective Sets of Security Upgrades

**5a. CONTRACT NO.**
HQ0034-14-D-0001

**5b. GRANT NO.**

**5c. PROGRAM ELEMENT NO(S).**

**6. AUTHOR(S)**
Kevin E. Burns, Jason A. Dechant, J. Darrell Morgeson, Yazmin Seda-Sanabria, Enrique E. Matheu

**5d. PROJECT NO.**

**5e. TASK NO.**
BA-6-3075

**5f. WORK UNIT NO.**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

**8. PERFORMING ORGANIZATION REPORT NO.**
IDA NS Document D-5324

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
U.S. Army Corps of Engineers, Headquarters
Office of Homeland Security
441 G Street NW (ATTN: CECW-HS)
Washington, DC 20314

**10. SPONSOR'S / MONITOR'S ACRONYM(S)**
USACE, HQ

**11. SPONSOR'S / MONITOR'S REPORT NO(S).**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Approved for public release; distribution is unlimited

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

The United States Army Corps of Engineers (USACE) conducts Security Risk Assessments (SRAs) at its most consequential dam projects. The Common Risk Model for Dams (CRM-D) provides a mathematically rigorous and easy-to-implement way to conduct SRAs. The CRM-D quantifies risk as the product of the probability of a successful attack and consequences. Referred to as conditional risk, this decision metric is the expected loss given a specified attack is attempted on a particular target. A specified attack (consisting of an attacker type and an attack vector) carried out on a particular target comprises a scenario.

The CRM-D considers three attacker types and 32 attack vectors identified by USACE Headquarters. A dam with only a modest number of critical assets could thus have several hundred scenarios and consequently several hundred conditional risk estimates. This paper introduces a decision metric, *exposure*, which allows the analyst to aggregate conditional risk estimates across scenarios. The analyst can use exposure to compare risks by attack type, by target or for any useful set of scenarios. These comparisons can guide an analyst in determining a proposed set of security upgrades. A standard set of graphics and return-on-investment calculations based on exposure are introduced that summarize the current level of risk at a dam project as well as the reduced level of risk should the set of recommended security upgrades be implemented.

**15. SUBJECT TERMS**
Risk assessment, dams sector, threat, vulnerability, consequences, exposure

**16. SECURITY CLASSIFICATION OF:**

| a. REPORT | b. ABSTRACT | c. THIS PAGE | 17. LIMITATION OF ABSTRACT | 18. NO. OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| U | U | U | UU | 20 | Jason A. Dechant |

**19b. TELEPHONE NUMBER (Include Area Code)**
(703) 845-2495